

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:

THE RESIDENCE LOCATED AT
210 BRIARIDGE DRIVE
TURTLE CREEK, PENNSYLVANIA 15145
AND ALL COMPUTERS AND CELLULAR
PHONES LOCATED THEREIN

18.1413M

Magistrate No.

[UNDER SEAL]

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Senior Special Agent David J. Halushka, being first duly sworn, hereby depose and state
as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **210 Briaridge Drive Turtle Creek, Pennsylvania 15145**, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B, both incorporated herein.

2. I am a Senior Special Agent with the United States Secret Service. I have been employed as a Special Agent since May 22, 2000. As a Special Agent, I have participated in criminal investigations to include the obtaining and execution of federal warrants. I have completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center as well as the Special Agent Training Course at the United States Secret Service James J. Rowley Training Center. I have also completed the Basic Computer Evidence Recovery Training and the Mobile Device Examiner training, specializing in computer and cellular phone forensics.

All of these programs provided training regarding Financial Crimes, Electronic Crimes, Fraud, and Criminal Investigations. Prior to joining the United States Secret Service I worked as an Attorney in the City of Pittsburgh from June of 1998 to May of 2000.

3. As a federal law enforcement officer, I am authorized to investigate violations of laws of the United States, including the crimes outlined herein, and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

5. This affidavit incorporates for reference the October 10, 2017 Application Under Rule 41 for a Warrant to Search and Seize the same PREMISES that was granted by this Court for evidence consistent with an identity theft and access device fraud investigation. Upon execution of said warrant, evidence was recovered that directly related to the manufacture of fraudulent credit cards and driver's licenses, as well as other evidence directly related to the compromise of personally identifiable information (PII). Items of evidence recovered included a laptop computer; cellular telephones; handwritten credit card numbers, dates of birth and social security numbers; gift cards; and credit cards in the names of persons who do not reside at the PREMISES.

6. This affidavit also incorporates for reference the July of 2016 search warrant executed by members of the Los Angeles Police Department (LAPD), the Federal Bureau of Investigation, and local law enforcement based on probable cause obtained during LAPD's investigation for a computer hacking investigation. LAPD had linked the hacking offenses and suspect IP address to the PREMISES. During the execution of the search warrant at the

PREMISES, an Apple desktop computer was recovered, among other items of evidence. A forensic exam of that computer revealed numerous documents containing PII within them to include contracts with financial information, credit applications, credit card numbers, social security numbers, passports, and other documents containing PII.

7. Those search warrants, and evidence gathered from other investigative means established that Quinyahta Rochelle has been, for many years, engaged in identity theft related offenses. During execution of both search warrants, law enforcement observed a device used to manufacture fraudulent credit cards.

8. Rochelle ultimately pleaded guilty to numerous federal offenses, including: Felon in Possession of a Firearm; Conspiracy to Knowingly Possess and Use the Means of Identification of Another Person and to Knowingly Use One or More Unauthorized Access Devices; Use of Unauthorized Access Devices (Counterfeit Ohio driver licensees); Wire Fraud; Aggravated Identity Theft; and Unauthorized Accessing Information from Protected Computers. She is currently on bond and awaiting sentencing.

9. The investigation and convictions followed from Rochelle's association with Albert McCall, who has since pleaded guilty to identity theft related offenses and fraud offenses. In summary, Rochelle provided McCall with credit reports that she obtained through the dark web (a private Internet browser) that she purchases using crypto-currency (Bitcoin). McCall also provided associates of Rochelle with Counterfeit Ohio driver licenses that Rochelle's associates would use, along with the PII of identity theft victims, to apply for credit at jewelry stores and other retail establishments. The PII was also used to rent hotel rooms and vehicles.

10. Rochelle has extremely limited legitimate employment. She is currently on bond pending her sentencing, and based on the evidence developed as described below, it appears that Rochelle has continued to commit identity theft related offenses while on bond.

11. In July of 2018, the United States Secret Service (USSS), Pittsburgh Field Office was contacted by local law enforcement concerning a credit card fraud investigation following \$4,000.00 in unauthorized charges on the reporting victim's LL Bean Visa credit card. Charges included purchases of Victoria Secret gift cards, gasoline, clothing and other miscellaneous items.

12. Video surveillance from a local gas station showed a black SUV, distinguishable by the brush guard on the front bumper and chrome accent trim, occupied by a black female who used a fraudulent credit card to purchase gasoline. The same credit card was used to purchase Victoria's Secret gift cards totaling \$1,450.00.

13. The gas station employee later observed the same vehicle backing into the driveway of 210 Briaridge Drive, Turtle Creek, PA. The employee captured a picture of the black SUV which is known to both local and federal law enforcement to be a Chevy Tahoe with Indiana license plates driven by Quinyahta Rochelle who resides at 210 Briaridge Drive, Turtle Creek, PA.

14. Continuing in July of 2018, the USSS was contacted by additional local law enforcement concerning a similar credit card fraud investigation in their jurisdiction. The victim reported that the victim's First Commonwealth Bank debit card was used to make numerous unauthorized purchases at various retail establishments over the course of several days.

15. Video surveillance obtained from several establishments show the same black Chevy Tahoe driven by a black female suspected to be Quinyahta Rochelle, including a Wendy's

drive-thru transaction where the suspect used the victim's debit card to pay for the food purchase. The victim's debit card was also used to purchase gasoline for the Chevy Tahoe.

16. In August of 2018, a trash pull was conducted at the PREMISES. One bag of trash was collected from the PREMISES but contained nothing of evidentiary value. Soon thereafter, information was received that a black female, driving a black Chevy SUV, was dumping her garbage in the dumpster at an apartment building near the PREMISES in the middle of the night, instead of leaving it out for trash at the PREMISES.

17. Based on my training and experience, and based on direct knowledge of this ongoing investigation, it appears that Rochelle is attempting to conceal items of evidence in her trash from being picked up by law enforcement while still leaving other trash items at the PREMISES for normal trash collection. Rochelle is aware that evidence was recovered from multiple trash pulls at the PREMISES during this ongoing investigation.

18. In September of 2018, USPIS was contacted by the Monroeville Police Department regarding counterfeit Chase Bank cards used at a Monroeville area Comfort Suites by an individual named Joseph Pallko. USPIS interviewed Pallko and he indicated that he received the cards from a woman named "Yahta" that lived on Briaridge Drive in Turtle Creek, PA and drove a black SUV. Pallko explained how "Yahta" would "clear" existing credit cards. (This is likely a reference to how she uses the magnetic stripe reader to delete the legitimate information on the back of bank cards.) A magnetic stripe reader has been found at her residence on previous search warrants.

19. Pallko stated that he visited "Yahta's" house on Briaridge Drive in Turtle Creek, PA and stated that he recalled her using her laptop in the kitchen/dining room area of the residence. Pallko confirmed that he heard "Yahta" on the phone with banks and told him that she called the

banks “to make sure it goes through.” Pallko confirmed that he used counterfeit credit cards that he received from “Yahta” at numerous hotels in the Pittsburgh, Pennsylvania area to reserve rooms for “Yahta.”

20. In October of 2018, USPIS and HSI interviewed CS1 connected to CS1’s use of counterfeit credit cards in the Pittsburgh area. CS1, who has an extensive criminal record, and another individual, were stopped by Monroeville Police in September of 2018 at a Jared’s Jewelers during an attempted use of a counterfeit credit/debit card.

21. At the time of the stop by Monroeville Police CS1 was in possession of two altered debit cards; one of which had “Joseph Pallko” embossed (stamped) on the front of the cards. In addition to the cards, CS1 was in possession of two handwritten post-it notes that contained PII and bank account information to two BB&T Bank customers. It should be noted that the handwriting on the post-it notes appear to be the same handwriting as that from the handwritten paper found in the search of the rental vehicle by Wilkins Township Police that Rochelle was a passenger.

22. During the interview with USPIS and HSI, CS1 related that they had purchased counterfeit cards and PII from an African American female nicknamed “the bank”, who drove a large black SUV. CS1 was shown a photo lineup that contained the photo of Quinyahta Rochelle. CS1 selected the photo of Rochelle and identified Rochelle as the individual known as “the bank”. CS1 provided the phone number “412-523-2611” for Rochelle.

23. The confidential source referenced in this affidavit and referred to as CS1 has been determined to be credible because the information provided has been corroborated through credit card and bank records and fraudulent credit and debit card transactions as well as through other

information obtained through the investigation. The information provided by CS1 also matches the method of operation that Rochelle has displayed in her prior cases with financial crimes.

24. USPIS obtained records from Chase Bank that identified approximately 60 compromised accounts with fraudulent transactions in the Pittsburgh, PA totaling approximately \$50,000.00 and further identified "412-523-2611" as one of the phone numbers that was used to contact the bank during the time of the fraudulent activity in order to obtain and/or edit account information.

25. The investigation has confirmed that the telephone number given by CS1 and captured by Chase Bank belongs to Quinyahta Rochelle. Furthermore, information developed throughout the ongoing investigations suggest that Rochelle routinely conducts these transactions in the PREMISES.

26. On October 22, 2018, the Wilkins Township Police Department conducted a traffic stop on a Chevy Tahoe. The vehicle, an Enterprise rental vehicle, was driven by Robert Mickens and had Quinyatha Rochelle as a passenger. Neither Mickens nor Rochelle was an authorized driver on the rental agreement. The vehicle was impounded and a search warrant was executed by Wilkins Township Police Department. Found in the vehicle were numerous Nordstrom gift cards; a piece of paper containing names, dates of birth, social security numbers and credit card numbers; and receipts for the purchase of Nordstrom gift cards totaling \$2,000.00. The gift card purchases were made with a credit card that matched one of the credit card numbers written on the piece of paper found in the vehicle that was in the name of "Kristin L (Keen-Varela)."

27. In addition to the above items listed that were found in the rental car, a Walmart receipt dated 10/14/18 for a Ria money transfer shows the receipt of \$1,800.00 from the money transfer service offered at the North Versailles, Pennsylvania Walmart location.

28. Your affiant received information from Walmart connected to Quinyahta Rochelle and her associated telephone number. Walmart provided information on fourteen (14) money transfer transactions between 9/6/17 and 6/18/18 totaling over \$16,000.00. Rochelle was the recipient in twelve (12) of those transactions, receiving almost \$13,000.00 from three (3) different senders. Rochelle sent over \$3,400.00 to a single recipient in two (2) separate transactions.

29. The information on the Walmart money transfer transactions is inconsistent with Rochelle's lack of employment history and further suggests her involvement in criminal activity.

30. A laptop computer in the vehicle at the time of the traffic stop was removed by Quinyahta Rochelle before the vehicle was impounded. Wilkins Township police confirmed that she took the laptop with her when she was driven home by Wilkins Township Police.

31. Through this ongoing investigation, which included various investigative techniques, it is known that Quinyahta Rochelle routinely utilizes her cellular phone and/or computer to obtain the compromised PII that she uses in furtherance of the fraudulent activity, including bank fraud, credit card fraud and aggravated identity theft. It is also known that she regularly keeps these devices at the PREMISES and that she normally conducts the fraudulent transactions in the PREMISES as well.

32. It is also known through this ongoing investigation that Quinyahta Rochelle regularly keeps items that she purchases by fraudulent means in the PREMISES.

33. It is also known through this ongoing investigation that Quinyahta Rochelle utilizes Bitcoin and/or other crypto-currency to purchase and/or sale compromised PII. Bitcoin transactions are recorded in the user's Bitcoin Wallet, accessible via either a computer or cellular telephone.

34. Agents confirmed through checking with the local post office through the United States Postal Inspection Service (USPIS) that Rochelle continues to receive her mail at the PREMISES.

TECHNICAL TERMS

35. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Cellular telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. Storage medium: A storage medium is any physical object upon which electronic data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

e. Bitcoin/Cryptocurrency: Bitcoin can be characterized as a “peer to peer” virtual currency that enables users to conduct transactions globally. The Bitcoin system is considered de-centralized because it operates with no central authority and transactions are effected via client software by users.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

36. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. Forms in which the records might be found could be data stored on a computer’s hard drive, cellular

phone, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

37. *Probable cause.* I submit that if a computer, cellular phone or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer, cellular phone or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or

applications, file system data structures, and virtual memory “swap” or paging files. Computer and/or cellular phone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

38. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers and/or cellular phones were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, mobile applications, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about

the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer, cellular phone or storage medium can also indicate who has used or controlled the computer, cellular phone or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer and/or a cellular phone works can, after examining this forensic evidence in its proper context, draw conclusions about how they were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or cellular phone is evidence may depend on other information stored on the computer or cellular phone and the application of knowledge about how they behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer or cellular phone[[to obtain unauthorized access to a victim's PII over the Internet]], the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer or cellular phone is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that a computer or cellular phone used to commit a crime of this type may contain: data that is evidence of how they were used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

39. *Necessity of seizing or copying entire computers, cellular phones or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers and cellular phones can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer and cellular phone hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

40. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying

storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

41. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

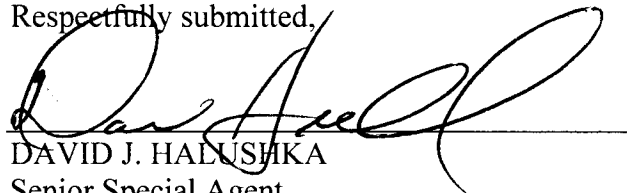
FORFEITURE

42. This application requests the issuance of a warrant under 21 U.S.C. § 853(f) authorizing the seizure of property subject to forfeiture. This is appropriate because: (1) there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture, and (2) an order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture. There is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture, because 18 U.S.C. § 1030(i)(1)(A) provides that the defendant's "interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation" shall be forfeited to the United States.

CONCLUSION

43. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "David J. Halushka", written over a horizontal line.

DAVID J. HALUSHKA
Senior Special Agent
United States Secret Service

Subscribed and sworn to before me
on October 31, 2018:

A handwritten signature in black ink, appearing to read "Robert C. Mitchell", written over a horizontal line.

HONORABLE ROBERT C. MITCHELL
United States Magistrate Judge

ATTACHMENT A

Property to be searched

The property to be searched is 210 Briaridge Drive, Turtle Creek, Pennsylvania 15145 and all computers located therein, further described as a single family dwelling with a paved driveway on right side of structure. The bottom/ground floor is constructed with brick and the top floor with a light in color vinyl siding. The structure has a brown roof, brown shutters, and a white front door.

Also to include any and all rooms, safes, attics, basements, and other parts therein and the surrounding grounds to include all garages, assigned storage areas, sheds, outbuildings and vehicles associated with 210 Briaridge Drive, Turtle Creek, Pennsylvania 15145, specifically a 2007 black Chevy Tahoe, VIN# 1GNFC13J17R220854, located at 210 Briaridge Drive, Turtle Creek, Pennsylvania 15145

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. 1028, 18 U.S.C. 1028A, and 18 U.S.C. 1030, including:

a. Person identification information, including social security numbers, dates of birth, account numbers, names, addresses, credit card numbers;

b. Any information related to First Commonwealth Bank, LL Bean, including credit card accounts and account number.

c. Evidence of recent purchases, including receipts, invoices, shipping documents, shipping boxes, and recently purchased merchandise;

d. Records and information relating to, including any attempt to access an Internet- based account related to any of the following individuals: Jennifer S. Mean, Stephanie A Werner, or Kristin L Keen-Varela;

e. Records and information relating to an access of internet based accounts held by victims of this investigation to include but not limited to Jennifer S. Mean, Stephanie A Werner, or Kristin L Keen-Varela;

f. Records and information relating to the e-mail accounts and attempts to gain access to e-mail accounts;

g. Records and information relating to Bitcoin or other cryptocurrency transactions related to the purchase and/or sale of compromised PII;

h. Records and information relating to the identity or location of the suspects, including travel records; and

- i. Records and information relating to malicious software.
2. Any and all machines, tools, materials, software, and or supplies used in the manufacturing or processing of counterfeit access devices.
3. Computers or storage media used as a means to commit the violations described above, including downloading confidential materials without authorization in violation of 18 U.S.C. § 1030(a)(2).
4. For any computer, cellular phone or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "DEVICE"):
 - a. Any of the evidence listed in 1(a) through 1(i) listed above;
 - b. evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - c. evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - d. evidence of the lack of such malicious software;
 - e. evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;
 - f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;

- g. evidence of the times the DEVICE was used;
- h. passwords, encryption keys, and other access devices that may be necessary to access the DEVICE;
- i. documentation and manuals that may be necessary to access the DEVICE or to conduct a forensic examination of the DEVICE;
- j. records of or information about Internet Protocol addresses used by the DEVICE;
- k. records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- l. contextual information necessary to understand the evidence described in this attachment.;
- m. All text messaging and emails and/or other records of communication by and between Quinyahta Rochelle and persons or entities that constitute the source of counterfeit credit cards or stolen credit card or financial institution information and/or the transfer of said information to other persons/entities for the period October 2017 through October 2018; and
- n. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, cloud data, and browsing history.

5. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.